CLAIMS

WHAT IS CLAIMED IS:

1. An intrusion detection and analysis system comprising:

a data monitoring device comprising a capture engine operable to capture data passing through the network and configured to monitor network traffic, decode protocols, and analyze received data;

an intrusion detection device comprising a detection engine operable to perform intrusion detection on data provided by the data monitoring device;

application program interfaces configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection; and

memory for storing reference network information used by the intrusion detection device to determine if an intrusion has occurred.

2. The system of claim 1 wherein the reference network information comprises a signature database including signature profiles associated with a known network security violation and wherein the detection engine is operable to compare the data provided by the data monitoring device with the signature profiles to detect network intrusions.

3. The system of claim 2 further comprising a parser operable to parse, generate, and load signatures at the detection engine.

4. The system of claim 1 wherein the reference network information comprises a baseline state of network traffic and wherein the detect engine is operable to compare the data received by the capture engine to the baseline network state and look for anomalies.

5. The system of claim 4 wherein the data monitoring device provides the baseline state of network traffic.

6. The system of claim 1 further comprising a log file configured to at least temporarily store reports generated by the detect engine.

7. The system of claim 6 further comprising an alarm manager operable to generate alarms based on information generated by the log file.

8. The system of claim 1 further comprising a filter configured to filter out packets received at the data monitoring device.

9. The system of claim 1 further comprising a statistics collector operable to collect statistics on packets received by the data monitoring device.

10. The system of claim 1 wherein the capture engine is configured to forward packets and temporarily store packets for later analysis by the data monitoring device.

11. A method for performing intrusion detection with an intrusion detection and analysis system comprising a data monitoring device configured to monitor network traffic, decode protocols, and analyze received data, and an intrusion detection device coupled to the data monitoring device and configured to perform intrusion detection on data provided by the data monitoring device; the method comprising:

receiving data at the data monitoring device;

capturing at least a portion of the packets contained within the data;

calling an application program interface configured to open applications of the data monitoring device; and

performing intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device.

12. The method of claim 11 wherein calling an application program interface comprises calling an application program interface configured to open a protocol decoding application.

13. The method of claim 11 wherein calling an application program interface comprises calling an application program interface configured to open an alarm generation application.

14. The method of claim 11 further comprising filtering the data prior to capturing packets.

15. The method of claim 11 wherein performing intrusion detection comprises performing signature matching.

16. The method of claim 15 wherein the application program interfaces provide parsing of signatures used in signature matching.

17. The method of claim 11 further comprising analyzing the data at the data monitoring device.

18. The method of claim 11 wherein performing intrusion detection comprises detecting anomalies in the received data.

19. A computer program product for performing intrusion detection with an intrusion detection and analysis system comprising a data monitoring device configured to monitor network traffic, decode protocols, and analyze received data, and an intrusion detection device coupled to the data monitoring device and configured to perform intrusion detection on data provided by the data monitoring device; the product comprising:

code that receives data at the data monitoring device;

code that captures at least a portion of the packets contained within the data;

code that calls an application program interface configured to open applications of the data monitoring device;

code that performs intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device; and

a computer-readable storage medium for storing the codes.

20. The computer program product of claim 19 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave.